УДК 351.746:007

СТРАТЕГІЧНІ РИЗИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ПРОГНОСТИКА КОРПОРАЦІЇ RAND

Макаренко Є.А.
доктор політичних наук, професор кафедри міжнародних медіакомунікацій і комунікативних технологій Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

Критичний аналіз стратегічних ризиків інформаційної безпеки був запропонований дослідниками у доповіді «Discontinuities and Distractions-Rethinking Security for the Year 2040» (2017 р.), яка містить прогнозування глобальних тенденцій у сфері безпеки та непередбачуваних подій, що можуть формувати світ на видиму перспективу. Оскільки прогностичні дослідження корпорації RAND сприймаються політичними лідерами і фаховими експертами різних країн як можливість екстраполяції певних тенденцій та їх наслідків на національному рівні, варто враховувати висновки документу для аналізу стратегій інформаційної безпеки на національному рівні функціонування міжнародних акторів.

Головною проблемою інформаційної і кібербезпеки у дослідженні було визначено перспективні порушення конфіденційності інформаційних ресурсів державного, корпоративного і приватного характеру, що можуть призвести до значного впливу деструктивних чинників на критично важливі сфери життєдіяльності суспільства, спричинити руйнування механізмів правового захисту інформаційної безпеки, викликати появу нових інформаційних загроз в умовах швидкоплинного технологічного прогресу, зниження якості інформації для урядів, що забезпечує ухвалення керівних рішень, зростання контенту, створеного за допомогою систем «штучного інтелекту», і водночас прискореного реагування на «фейкові» повідомлення [1].

У доповіді зазначається, що ризики глобалізації можуть мати політичний, правовий, фінансово-економічний, соціокультурний, безпековий та гуманітарний характер. Політичний ризик дослідники пов’язують з політичними діями та міжнародною діяльністю урядів іноземних країн. Такі кризи, як терористичні напади 11 вересня 2001 р. у США, триваючі конфлікти в Сирії, Іраку, Пакистані, Лівії та інших країнах, нестабільність на Корейському півострові і фінансові кризи зробили геополітичну невизначеність ключовим компонентом формування глобальної стратегії. Вплив цих подій та пов’язаних з ними політичних

рішень щодо енергетики, транспорту, туризму, страхування та інших секторів демонструє масові наслідки війн та економічних криз, де б вони не відбувалися. Оцінка політичного ризику передбачає оцінку стабільності поточного уряду країни та її відносин з іншими країнами. Високий рівень ризику впливає на право власності на фізичні активи та інтелектуальну власність, а також на безпеку спільноти, що збільшує потенціал для кризової ситуації. На думку експертів корпорації RAND, політичні ризики поділяються на дві підкатегорії: глобальні ризики і ризики для конкретної країни. Глобальні ризики впливають на всі багатонаціональні операції міжнародних акторів і корпорацій, натомість ризики для конкретної країни пов'язані з інвестиціями в певну іноземну країну.

Фінансово-економічні ризики спричиняють нестабільність макроекономічних показників країни та здатність країн виконувати свої фінансові зобов'язання і безпосередньо впливають на результативність їхньої життєдіяльності. Конкурентоспроможність і коливання валюти в країні, йдеться у доповіді, є важливими показниками стабільності країни як фінансової, так і політичної та її готовності прийняти зміни та інновації. Крім того, оцінка фінансового ризику повинна враховувати такі чинники, як рівень управління економікою, рівень економічного розвитку країни, умови праці, інфраструктура, технологічні інновації та наявність природних та людських ресурсів.

Соціально-культурні ризики пов'язані з діяльністю в іншому соціокультурному середовищі і стосуються конкретних ідеологій, відносного значення етнічних, релігійних та націоналістичних рухів, здатності країни сприйняти зміни, які рано чи пізно будуть спричинені іноземними впливами. Такі елементи, як рівень життя, патріотизм, релігійні фактори або наявність харизматичних лідерів, можуть відіграти значну роль в оцінці цих ризиків.

Стратегічні ризики інформаційної безпеки пов'язуються зі стрімким розвитком цифрових технологій, використанням штучного інтелекту у сфері безпеки, вдосконаленням інформаційних озброєнь та застосуванням деструктивних впливів у протиборстві. Стратегічна парадигма інформаційної безпеки, яка стосується всіх верств суспільства, слугує для забезпечення інформаційного суверенітету, безпеки і надійності національної інформаційної інфраструктури, конфіденційності інформаційних ресурсів і приватного життя, тобто практично виступає як модель вирішення проблеми інформаційної безпеки у зовнішньому і внутрішньому політичному середовищі. Фахівці вважають, що національні стратегії інформаційної безпеки мають ґрунтуватися на врахуванні динамічних змін сучасної політичної реальності, еволюції концепцій сили у міжнародних відносинах та впровадженні механізмів забезпечення

національної інформаційної безпеки як складової зовнішньої і безпекової політики. прискореного реагування на «фейкові» повідомлення [2-4].

Інноваційні можливості високих технологій мають неоднозначні наслідки для інформаційної безпеки України, оскільки вони впливають на сферу безпеки і оборони держави, демократизацію державного управління, відкривають можливості для вирішення кризових ситуацій, забезпечують протидію деструктивній пропаганді, а також спричиняють маргіналізацію окремих верств суспільства у сучасному розвитку країни. За умов функціонування глобальної мережевої інфраструктури інформаційна та кібербезпека набуває пріоритетного значення для ефективної безпекової політики загалом, впливає на характер і засоби реалізації національних інтересів у глобальному інформаційному середовищі, на діяльність традиційних політичних інститутів, а також на процеси формування громадської думки.

З'ясування потенційних ризиків у сфері інформаційної безпеки важливе для окреслення їх характерних особливостей та засобів використання у контексті просування пріоритетних інтересів України на міжнародній арені і для переконання світової громадськості й внутрішньої спільноти у правильності рішень політичних та безпекових інститутів щодо захисту базових пріоритетів держави. Особливої актуальності і повсюдної практичної значимості у сфері інформаційної безпеки набувають статусні комунікації, які відіграють все більш домінуючу роль в різних сферах життєдіяльності України, оскільки не тільки відображають події реального світу, а й самі впливають на перебіг безпекових процесів у видимій перспективі.

Список використаних джерел

1. Hoehn A. R., Parasiliti A., Efron S., Strongin S. Discontinuities and Distractions—Rethinking Security for the Year 2040 [Електронний ресурс] – Режим доступу: https://www.rand.org/pubs/conf_proceedings/CF384.html

2. Global Strategy and Risk [Електронний ресурс] – Режим доступу: https://saylordotorg.github.io/text_fundamentals-of-global-strategy/s03-06-global-strategy-and-risk.html

3. 2019 Global Cyber Risk Perception Survey[Електронний ресурс] – Режим доступу: https:// www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf

4. Cavelty M. D., Egloff F. J. The Politics of Cybersecurity: Balancing Different Roles of the State [Електронний ресурс] – Режим доступу: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities studies/ pdfs/ Dunn_ Cavelty_ Egloff_ 2019% 20STAIR %20Issue%2015.1.pdf